FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **112740-274**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **09/914109**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE00/00492	**22 February 2000**	**23 February 1999**

TITLE OF INVENTION
METHOD AND APPARATUS FOR USER IDENTIFICATION

APPLICANT(S) FOR DO/EO/US
Manfred Bromba

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☒ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

Submission of Drawings - Figures 1-3 on three sheets

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/914109	PCT/DE00/00492	112740-274

21. The following fees are submitted:	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :		
☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1,000.00**		
☒ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO **$860.00**		
☐ International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	**$860.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	19 - 20 =	0	x	$18.00	**$0.00**
Independent claims	2 - 3 =	0	x	$80.00	**$0.00**
Multiple Dependent Claims **(check if applicable)**.			☐		**$0.00**
TOTAL OF ABOVE CALCULATIONS				=	**$860.00**
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.				☐	**$0.00**
SUBTOTAL				=	**$860.00**
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).				+	**$0.00**
TOTAL NATIONAL FEE				=	**$860.00**
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**				☐	**$0.00**
TOTAL FEES ENCLOSED				=	**$860.00**
					Amount to be: refunded $
					charged $

☒ A check in the amount of **$860.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **02-1818** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

William E. Vaughan (Reg. No. 39,056)
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690

SIGNATURE

William E. Vaughan
NAME

39,056
REGISTRATION NUMBER

August 23, 2001
DATE

BOX PCT

IN THE UNITED STATES ELECTED/DESIGNATED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

PRELIMINARY AMENDMENT

APPLICANT:	Manfred Bromba	DOCKET NO.:	112740-274
SERIAL NO:		GROUP ART UNIT:	
FILED:		EXAMINER:	
INTERNATIONAL APPLICATION NO.		PCT/DE00/00492	
INTERNATIONAL FILING DATE:		February 22, 2000	
INVENTION:	METHOD AND APPARATUS FOR USER IDENTIFICATION		

Assistant Commissioner for Patents,
Washington, D.C. 20231

Sir:

Please amend the above-identified International Application before entry into the National stage before the U.S. Patent and Trademark Office under 35 U.S.C. §371 as follows:

In the Specification:

Please replace the Specification of the present application, including the Abstract, with the following Substitute Specification:

SPECIFICATION

TITLE

METHOD AND APPARATUS FOR USER IDENTIFICATION

BACKGROUND OF THE INVENTION

The present invention relates to a method and an apparatus for user identification for the unambiguous identification of a user or subscriber to a system.

Such a system can be, for example, a terminal such as a mobile telephone, or a building to which only certain persons should have access. However, it also can be a computer network which only allows access to certain data after unambiguous identification of the user; for example in on-line banking.

It is known that the user identifies oneself by a personal identification number (PIN) only known to the user in the ideal case. However, this method has the disadvantage that the user can easily forget or mistake the number due to the multiplicity of numbers to be used. The PIN number is, therefore, frequently noted in notebooks or the like which, however, entails a security risk.

For this reason, biometric identification methods recently have been developed in which biometric features of a user are used for the authentication. Such a biometric identification is a method for ensuring the allocation and the access of a certain person to a system or a location, which is not simple but is convenient and often very secure. Compared with the PIN code, the biometric identification has the advantage that it cannot be forgotten and the biometric features can be copied only by very elaborate measures or not at all. This is because, whereas the PIN code is pure software, there is always a more or less unambiguous correlation with the hardware, i.e. with the body of the respective user, in the case of biometric features. A possibility of such a biometric identification consists in the acquisition of the fingerprint of a finger of the user. The user places, for example, the right-hand thumb onto a contact area of an input device where the fingerprint patterns are detected with a resolution of approximately 50 μm. A computer unit compares the acquired fingerprint features such as branches or minuscules with the features of stored fingerprints of persons authorized for access. If there is a certain degree of correspondence which allows unambiguous identification of the user with very high probability, then use is allowed.

The problem with such fingerprint recognition systems is, however, that the finger, especially if it is contaminated, leaves traces on the sensor in the form of the fingerprint which, under certain conditions, can lead to recognition of the same authorized person during a new access authorization check without the finger having been applied again. For example, it is conceivable that using a glove or the like, pressure is exerted on the fingerprint sensor with the traces of the finger of the preceding authorized user and thus the authorized user is recognized again. This can result in possible misuse of the user identification.

The present invention is, therefore, directed to a method and apparatus for user identification using biometric data, particularly fingerprint data, in which an erroneous identification due to remaining traces of a preceding identification process is prevented.

Such object is achieved by an identification method having the following steps:

(I) acquisition of a biometric record of the user and the respective spatial position of the biometric data relative to a reference position;

(II) storage of the biometric record and the associated position data;

(III) reading out the biometric record and the associated position data of an identification process preceding the current identification process; and

(IV) comparison of the biometric data currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric data have a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range.

The present invention is based on the fact that, as a rule, a user is not able to position his finger during a new placement on the sensor with an accuracy of less than 100 μm in the vertical and horizontal direction. If a corresponding fingerprint with corresponding position is acquired during two successive identification processes, it is assumed that in the second identification process, the print traces remaining from the preceding identification process are being misused and access authorization is refused.

In an advantageous embodiment of the method of the present invention, a mean value of the positions of a number of individual features of the biometric data is determined during the acquisition of the biometric record and, during the position comparison check of two successive identification processes, these mean position values are compared with one another. Since the mean values are subject to less spread, for example due to a stretching or compression of the surface of the skin or because of the acquisition raster of the pickup device, the tolerance range in which a position correspondence is evaluated as misuse, can be selected to be narrower in this variant of the method so that unwanted nonrecognition of a finger placed down correctly twice in succession becomes more improbable.

Additional features and advantages of the present invention are describe in, and will be apparent from, the following detailed description of the invention and the figures.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 shows a diagrammatic block diagram of an exemplary embodiment of the apparatus according to the present invention.

Figure 2 shows a flowchart explaining an exemplary embodiment of the method according to the present invention.

Figure 3 shows a flowchart explaining a further exemplary embodiment of the method according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Referring to Figure 1, a fingerprint sensor 1 has a contact area 5 for placing a finger (indicated in dashed lines) and acquires the features such as branches or minuscules of the fingerprint. A position acquisition device 2 acquires the positions of these features relative to a reference position; for example, a coordinate origin of an xy coordinate system of the contact area 5. The fingerprint data and associated position information thus determined are supplied to a memory 3 and a comparison device 4. From the memory 3, the corresponding fingerprint data and position data of the preceding fingerprint acquisition are read out and also supplied to the comparison device 4. The fingerprint features and their positions are compared there and, in the case of a correspondence which is within a tolerance range, the comparison device 4 evaluates the current fingerprint acquisition or, respectively, the current identification process as misuse of fingerprint traces of the last identification process and rejects access which is indicated on a display device 6.

In this method, the present invention is based on the fact that

(1) old fingerprint traces are no longer of consequence when a new arbitrary finger is placed on the area, and are replaced by the new print, and

(2) a user will not be able to position his finger, when placing it down again, with such accuracy that the finger corresponds to the preceding fingerprint within up to 100 µm or 50 µm in position and direction.

Since the position of the remaining traces of the earlier fingerprint of the preceding identification process cannot shift in space with respect to the sensor, it is not only the individual features of the fingerprint such as branches or minuscules but also their precise position on the contact area which are stored in the present invention; for example, as xy coordinates or as polar coordinates. If, in the case of a new fingerprint of a new identification process, corresponding features lie within a tolerance range of 50 µm or 100 µm at the same spatial position, it is highly probable that this is not a new placement of a finger of the same person but the features of the

last print. In this case, access authorization or identification must be refused and the user must be requested to place his/her finger again.

An exemplary embodiment of the method according to the present invention will now be explained with reference to the flowchart of Figure 2.

In a step S1, the biometric data and their associated positions on the contact area are acquired. In a step S2 these are stored for use in the user identification process following next. In step 3, accordingly, the biometric data and associated positions of the preceding identification process are read out. In step S4, a comparison is made to determine whether the features and positions of the two successive acquisitions, i.e. the fingerprint acquisition of the current user identification process and the fingerprint acquisition of the immediately preceding user identification process, correspond with each other. If both the features of the fingerprint have a defined degree of correspondence and the positions of these features correspond to one another within a tolerance range of 50 µm or 100 µm, the identification is refused (step S5). Otherwise, the check continues to step S6 in which a check is made, as in known user identification methods, to determine whether the features of the current acquisition of the fingerprint correspond to the stored features of fingerprints of certain persons; for example, authorized users. If this is not so, identification is refused (step S7). Otherwise, identification takes place.

The variant of the method explained in Figure 3 differs from that shown in Figure 2 in that a mean value of the positions of acquired features of the biometric record (fingerprint) is calculated and stored in a step S11. In step S4, it is then not the positions of individual features of the fingerprints but the mean position values of the current fingerprint acquisition and the preceding one which are compared with one another. This has the advantage that statistic deviations due to stretching or compression of the skin or due to the pixel spacing of the contact area 5 of the fingerprint sensor are averaged out so that the tolerance range can be selected to be smaller; for example, 10 µm to 20 µm. This reduces the probability of unjustified rejections of the identification.

The present invention provides an improved method for biometric user identification in which misuse due to fingerprint traces of a preceding user identification which are remaining on the acquisition device can be prevented. The present invention can be applied to checking the authorization to use devices such as,

for example, mobile telephones or for identifying a computer user in bank transactions. However, other applications also are conceivable in which the identity of a person must be reliably established on the basis of biometric data such as, for example, a fingerprint.

Although the present invention has been described with reference to specific embodiments, those of skill in the art will recognize that changes may be made thereto without departing from the spirit and the scope of the invention as set forth in the hereafter appended claims.

ABSTRACT OF THE DISCLOSURE

A method and apparatus for user identification involving:

(1) acquisition of a biometric record, preferably fingerprint data, of the user and the respective spatial position of the biometric data relative to a reference position;

(2) storage of the biometric record and the associated position data;

(3) reading out the biometric record and the associated position data of a user identification process preceding the current user identification process; and

(4) comparison of the biometric record currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric record has a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range.

In the claims:

On page 8, cancel line 1, and substitute the following left-hand justified heading therefor:

CLAIMS

Please cancel claims 1-16 without prejudice, and substitute the following claims therefore:

17. A method for biometric identification of a user, the method comprising the steps of:

acquiring, in a current user identification process, both a biometric record of the user and associated spatial position data of the biometric record relative to a reference position;

storing both the biometric record and the associated spatial position data;

reading out both a preceding biometric record and preceding associated spatial position data of a preceding user identification process which precedes the current user identification process;

comparing the biometric record currently acquired and the associated spatial position data with the preceding biometric record and the associated spatial position data read out; and

rejecting the identification of the user if there is a defined degree of correspondence between the biometric record currently acquired and the preceding biometric record, and the spatial position data currently acquired is within a defined tolerance range from the preceding spatial position data.

18. A method for biometric identification of a user as claimed in Claim 17, wherein the tolerance range is less than 100 μm.

19. A method for biometric identification of a user as claimed in Claim 17, wherein the tolerance range is approximately 50 μm.

20. A method for biometric identification of a user as claim in Claim 17, the method further comprising the steps of:

determining a mean value of positions of a plurality of individual features of the biometric record in each user identification process; and

using the mean values of two successive user identification processes in the step of comparing.

21. A method for biometric identification of a user as claimed in Claim 20, wherein the tolerance range is less than 50 μm.

22. A method for biometric identification of a user as claimed in Claim 20, wherein the tolerance range is between 10 μm and 20 μm.

23. A method for biometric identification of a user as claimed in Claim 17, wherein the biometric record is fingerprint data.

24. A method for biometric identification of a user as claimed in Claim 23, the method further comprising the step of:

determining, as the spatial position data, coordinates of at least one of branches and minuscules of the fingerprint on a contact area.

25. A method for biometric identification of a user as claimed in Claim 17, the method further comprising the steps of

deleting, after a user identification process has ended, the stored biometric record in the associated spatial position data of the preceding identification process; and

overriding the previously stored biometric record and the associated spatial position data of the preceding identification process with the biometric record and the associated spatial position data of the current identification process.

26. An apparatus for biometric identification of a user, comprising;

a device for acquiring, in a current user identification process, both a biometric record of the user and associated spatial position data of the biometric record relative to a reference position;

a memory for storing both the biometric record and the associated spatial position data; and

a comparison device for comparing the biometric record currently acquired and the associated spatial position data with a preceding biometric record and preceding associated spatial position data of a preceding user identification process, and for rejecting the identification of the user if there is a defined degree of correspondence between the biometric record currently acquired and the preceding biometric record, and the spatial position data currently acquired is within a defined tolerance range from the preceding spatial identification data.

27. An apparatus for biometric identification of a user as claimed in Claim 26, further comprising:

an output device for outputting a result of the user identification process.

28. An apparatus for biometric identification of a user as claimed in Claim 26, wherein the tolerance range is less than 100 μm.

29. An apparatus for biometric identification of a user as claimed in Claim 26, wherein the tolerance range is approximately 50 μm.

30. An apparatus for biometric identification of a user as claimed in Claim 26, further comprising:

a device for calculating a mean value of positions of a plurality of individual features of the biometric record in each user identification process, wherein the comparison device compares the mean values of two successive user identification processes.

31. An apparatus for biometric identification of a user as claimed in Claim 30, wherein the tolerance range is less than 50 μm.

32. An apparatus for biometric identification of a user as claimed in Claim 30, wherein the tolerance range is between 10 μm and 20 μm.

33. An apparatus for biometric identification of a user as claimed in Claim 26, further comprising:

a fingerprint sensor for acquiring a fingerprint as the biometric record and the associated spatial position data on a contact area of the fingerprint sensor.

34. An apparatus for biometric identification of a user as claimed in Claim 33, wherein the fingerprint sensor determines coordinates of certain features of the fingerprint on the contact area.

35. An apparatus for biometric identification of a user as claimed in Claim 34, wherein the certain features of the fingerprint are at least one of branches and minuscules.

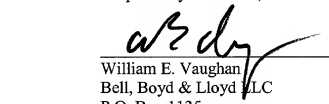
REMARKS

The present amendment makes editorial changes and corrects typographical errors in the specification, which includes the Abstract, in order to conform the specification to the requirements of United States Patent Practice. No new matter is added thereby. Attached hereto is a marked-up version of the changes made to the specification by the present amendment. The attached page is captioned **"Version With Markings To Show Changes Made".**

In addition, the present amendment cancels original claims 1-16 in favor of new claims 17-35. Claims 17-35 have been presented solely because the revisions by red-lining and underlining which would have been necessary in claims 1-16 in order to present those claims in accordance with preferred United States Patent Practice would have been too extensive, and thus would have been too burdensome. The present amendment is intended for clarification purposes only and not for substantial reasons related to patentability pursuant to 35 U.S.C. §§103, 102, 103 or 112. Indeed, the cancellation of claims 1-16 does not constitute an intent on the part of the Applicants to surrender any of the subject matter of claims 1-16.

Early consideration on the merits is respectfully requested.

Respectfully submitted,



(Reg. No. 39,056)

William E. Vaughan
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690-1135
(312) 807-4292
Attorneys for Applicants

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In The Specification:

The Specification of the present application, including the Abstract, has been amended as follows:

SPECIFICATION

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR USER IDENTIFICATION

~~**Description**~~

~~**User identification method**~~

BACKGROUND OF THE INVENTION

The present invention relates to a method and ~~a device~~ an apparatus for user identification for the unambiguous identification of a user or subscriber to a system.

Such a system can be, for example, a terminal such as a mobile telephone, or a building to which only certain persons should have access. However, it ~~can~~ also can be a computer network which only allows access to certain data after unambiguous identification of the user~~;~~, for example in on-line banking.

It is known that the user identifies ~~himself~~ oneself by a personal identification number (PIN) only known to ~~him~~ the user in the ideal case. However, this method has the disadvantage that the user can easily forget or mistake the number due to the multiplicity of numbers to be used. The PIN number is, therefore, frequently noted in notebooks or the like which, however, entails a security risk.

For this reason, biometric identification methods recently have been ~~recently~~ developed in which biometric features of a user are used for the authentication. Such a biometric identification is a method for ensuring the allocation and the access of a certain person to a system or a location, which is not simple but is convenient and often very secure. Compared with the PIN code, the biometric identification has the advantage that it cannot be forgotten and the biometric features can be copied only by very elaborate ~~means~~ measures or not at all. This is because, whereas the PIN code is pure software, there is always a more or less unambiguous correlation with the hardware, i.e. with the body of the respective user, in the case of biometric features. A possibility of such a biometric identification consists in the acquisition of the fingerprint of a finger of the user. The ~~latter~~ user places, for example, the right-hand

thumb onto a contact area of an input device where the fingerprint patterns are detected with a resolution of approximately 50 µm. A computer unit compares the acquired fingerprint features such as branches or minuscules with the features of stored fingerprints of persons authorized for access. If there is a certain degree of correspondence which allows unambiguous identification of the user with very high probability, then use is allowed.

The problem with such fingerprint recognition systems is, however, that the finger, especially if it is contaminated, leaves traces on the sensor ~~traces~~ in the form of the fingerprint which, under certain conditions, can lead to recognition of the same authorized person during a new access authorization check without the finger having been applied again. For example, it is conceivable that using a glove or the like, pressure is exerted on the fingerprint sensor with the traces of the finger of the preceding authorized user and thus the authorized user is recognized again. This can result in possible misuse of the user identification.

The present invention is, therefore, ~~based on the object of proposing~~ directed to a method and apparatus for user identification ~~by means of~~ using biometric data, particularly fingerprint data, in which an erroneous identification due to remaining traces of a preceding identification process is prevented.

~~The~~ Such object is achieved by an identification method having the following steps:

(I) acquisition~~(I) Acquisition~~ of a biometric record of the user and the respective spatial position of the biometric data relative to a reference position~~,~~;

(II) ~~Storage~~ storage of the biometric record and the associated position data~~,~~;

(III) ~~Reading~~ reading out the biometric record and the associated position data of an identification process preceding the current identification process; and~~,~~

(IV) ~~Comparison~~ comparison of the biometric data currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric data have a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range.

The present invention is based on the fact that, as a rule, a user is not able to position his finger during a new placement on the sensor with an accuracy of less than

100 μm in the vertical and horizontal direction. If a corresponding fingerprint with corresponding position is acquired during two successive identification processes, it is assumed that in the second identification process, the print traces remaining from the preceding identification process are being misused and access authorization is refused.

~~The invention also proposes a device for biometric user identification having the features of claim 8. Advantageous further developments of the method according to the invention and of the device according to the invention are described in the subclaims.~~

~~In an advantageous further development of the method~~ In an advantageous embodiment of the method of the present invention, a mean value of the positions of a number of individual features of the biometric data is determined during the acquisition of the biometric record and, during the position comparison check of two successive identification processes, these mean position values are compared with one another. Since the mean values are subject to less spread, for example due to a stretching or compression of the surface of the skin or because of the acquisition raster of the pickup device, the tolerance range in which a position correspondence is evaluated as misuse, can be selected to be narrower in this variant of the method so that unwanted nonrecognition of a finger placed down correctly twice in succession becomes more improbable.

BRIEF DESCRIPTION OF THE FIGURES

~~In the text which follows, the invention will be explained in detail by means of exemplary embodiments and referring to the drawings, in which~~

Figure 1 shows a diagrammatic block diagram of an exemplary embodiment of the ~~device~~ apparatus according to the present invention~~,~~.

Figure 2 shows a flowchart explaining an exemplary embodiment of the method according to the present invention~~, and~~.

Figure 3 shows a flowchart explaining a further exemplary embodiment of the method according to the ~~invention.~~ present invention.

~~Firstly, an exemplary embodiment of the invention will be explained with reference to the block diagram in Figure 1.~~

DETAILED DESCRIPTION OF THE INVENTION

~~A~~ Referring to Figure 1, a fingerprint sensor 1 has a contact area 5 for placing a finger (indicated in dashed lines) and acquires the features such as branches or minuscules of the fingerprint. A position acquisition device 2 acquires the positions of these features relative to a reference position~~,~~; for example, a coordinate origin of an xy coordinate system of the contact area 5. The fingerprint data and associated position information thus determined are supplied to a memory 3 and a comparison device 4. From the memory 3, the corresponding fingerprint data and position data of the preceding fingerprint acquisition are read out and also supplied to the comparison device 4. The fingerprint features and their positions are compared there~~,~~ and, in the case of a correspondence which is within a tolerance range, the comparison device 4 evaluates the current fingerprint acquisition or, respectively, the current identification process as misuse of fingerprint traces of the last identification process and rejects access which is indicated on a display device 6.

In this method, the present invention is based on the fact that

(1) old fingerprint traces are no longer of consequence when a new arbitrary finger is placed on the area, and are replaced by the new print, and

(2) a user will not be able to position his finger, when placing it down again, with such accuracy that the finger corresponds to the preceding fingerprint within up to 100 μm or 50 μm in position and direction.

Since the position of the remaining traces of the earlier fingerprint of the preceding identification process cannot shift in space with respect to the sensor, it is not only the individual features of the fingerprint such as branches or minuscules but also their precise position on the contact area which are stored in the present invention~~,~~; for example, as xy coordinates or as polar coordinates. If, in the case of a new fingerprint of a new identification process, corresponding features lie within a tolerance range of 50 μm or 100 μm at the same spatial position, it is highly probable that this is not a new placement of a finger of the same person but the features of the last print. In this case, access authorization or identification must be refused and the user must be requested to place ~~his~~ his/her finger again.

An exemplary embodiment of the method according to the present invention will now be explained with reference to the flowchart of ~~figure~~ Figure 2.

In a step S1, the biometric data and their associated positions on the contact area are acquired. In a step S2 these are stored for use in the user identification process following next. In step 3, accordingly, the biometric data and associated positions of the preceding identification process are read out. In step S4, a comparison is made to determine whether the features and positions of the two successive acquisitions, i.e. the fingerprint acquisition of the current user identification process and the fingerprint acquisition of the immediately preceding user identification process, correspond with each other. If both the features of the fingerprint have a defined degree of correspondence and the positions of these features correspond to one another within a tolerance range of 50 µm or 100 µm, the identification is refused (step S5)~~, otherwise.~~ Otherwise, the check continues to step S6 in which a check is made, as in known user identification methods, to determine whether the features of the current acquisition of the fingerprint correspond to the stored features of fingerprints of certain persons~~;~~, for example, authorized users. If this is not so, identification is refused (step S7)~~, otherwise.~~ Otherwise, identification takes place.

The variant of the method explained in ~~figure~~ Figure 3 differs from that shown in ~~figure 2~~ Figure 2 in that a mean value of the positions of acquired features of the biometric record (fingerprint) is calculated and stored in a step S11. In step S4, it is then not the positions of individual features of the fingerprints but the mean position values of the current fingerprint acquisition and the preceding one which are compared with one another. This has the advantage that statistic deviations due to stretching or compression of the skin or due to the pixel spacing of the contact area 5 of the fingerprint sensor are averaged out so that the tolerance range can be selected to be smaller~~;~~, for example, 10 µm to 20 µm. This reduces the probability of unjustified rejections of the identification.

The present invention provides an improved method for biometric user identification in which misuse due to fingerprint traces of a preceding user identification which are remaining on the acquisition device can be prevented. The present invention can be applied to checking the authorization to use devices such as, for example, mobile telephones or for identifying a computer user in bank transactions. However, other applications ~~are~~ also are conceivable in which the identity of a person must be reliably established on the basis of biometric data such as, for example, a fingerprint.

~~Abstract~~

~~User identification method~~

ABSTRACT

A method and apparatus for ~~biometric~~ user identification ~~exhibits the following steps:~~ involving:

~~(1) Acquisition~~(1) acquisition of a biometric record, preferably fingerprint data, of the user and the respective spatial position of the biometric data relative to a reference position~~,~~;

(2) ~~Storage~~ storage of the biometric record and the associated position data~~,~~;

(3) ~~Reading~~ reading out the biometric record and the associated position data of a user identification process preceding the current user identification process; and~~,~~

(4) ~~Comparison~~ comparison of the biometric ~~data~~ record currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric ~~data have~~ record has a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range. ~~The biometric data are preferably fingerprint data.~~

~~(Figure 2)~~

3/pats

Description

User identification method

The invention relates to a method and a device for user identification for the unambiguous identification of a user or subscriber to a system.

Such a system can be, for example, a terminal such as a mobile telephone, or a building to which only certain persons should have access. However, it can also be a computer network which only allows access to certain data after unambiguous identification of the user, for example in on-line banking.

It is known that the user identifies himself by a personal identification number (PIN) only known to him in the ideal case. However, this method has the disadvantage that the user can easily forget or mistake the number due to the multiplicity of numbers to be used. The PIN number is, therefore, frequently noted in notebooks or the like which, however, entails a security risk.

For this reason, biometric identification methods have been recently developed in which biometric features of a user are used for the authentication. Such a biometric identification is a method for ensuring the allocation and the access of a certain person to a system or a location, which is not simple but is convenient and often very secure. Compared with the PIN code, the biometric identification has the advantage that it cannot be forgotten and the biometric features can be copied only by very elaborate means or not at all. This is because, whereas the PIN code is

pure software, there is always a more or less unambiguous correlation with the hardware, i.e. with the body of the respective user, in the case of biometric features. A possibility of such a

biometric identification consists in the acquisition of the fingerprint of a finger of the user. The latter places, for example, the right-hand thumb onto a contact area of an input device where the fingerprint patterns are detected with a resolution of approximately 50 µm. A computer unit compares the acquired fingerprint features such as branches or minuscules with the features of stored fingerprints of persons authorized for access. If there is a certain degree of correspondence which allows unambiguous identification of the user with very high probability, then use is allowed.

The problem with such fingerprint recognition systems is, however, that the finger, especially if it is contaminated, leaves on the sensor traces in the form of the fingerprint which, under certain conditions, can lead to recognition of the same authorized person during a new access authorization check without the finger having been applied again. For example, it is conceivable that using a glove or the like, pressure is exerted on the fingerprint sensor with the traces of the finger of the preceding authorized user and thus the authorized user is recognized again. This can result in possible misuse of the user identification.

The invention is, therefore, based on the object of proposing a method for user identification by means of biometric data, particularly fingerprint data, in which an erroneous identification due to remaining traces of a preceding identification process is prevented.

The object is achieved by an identification method having the following steps

(I) Acquisition of a biometric record of the user and the respective spatial position of the biometric data relative to a reference position,

(II) Storage of the biometric record and the associated position data,

(III) Reading out the biometric record and the associated position data of an identification process preceding the current identification process,

(IV) Comparison of the biometric data currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric data have a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range.

The invention is based on the fact that, as a rule, a user is not able to position his finger during a new placement on the sensor with an accuracy of less than 100 µm in the vertical and horizontal direction. If a corresponding fingerprint with corresponding position is acquired during two successive identification processes, it is assumed that in the second identification process, the print traces remaining from the preceding identification process are being misused and access authorization is refused.

The invention also proposes a device for biometric user identification having the features of claim 8. Advantageous further developments of the method according to the invention and of the device according to the invention are described in the subclaims.

In an advantageous further development of the method, a mean value of the positions of a number of individual features of the biometric data is determined during the acquisition of the biometric record and, during the position comparison check of two successive identification processes, these mean position values

are compared with one another. Since the mean values are subject to less spread, for example due to a stretching or

compression of the surface of the skin or because of the acquisition raster of the pickup device, the tolerance range in which a position correspondence is evaluated as misuse, can be selected to be narrower in this variant of the method so that unwanted nonrecognition of a finger placed down correctly twice in succession becomes more improbable.

In the text which follows, the invention will be explained in detail by means of exemplary embodiments and referring to the drawings, in which

Figure 1 shows a diagrammatic block diagram of an exemplary embodiment of the device according to the invention,

Figure 2 shows a flowchart explaining an exemplary embodiment of the method according to the invention, and

Figure 3 shows a flowchart explaining a further exemplary embodiment of the method according to the invention.

Firstly, an exemplary embodiment of the invention will be explained with reference to the block diagram in Figure 1.

A fingerprint sensor 1 has a contact area 5 for placing a finger (indicated in dashed lines) and acquires the features such as branches or minuscules of the fingerprint. A position acquisition device 2 acquires the positions of these features relative to a reference position, for example a coordinate origin of an xy coordinate system of the contact area 5. The fingerprint data and associated position information thus determined are supplied to a memory 3 and a comparison device 4. From the memory 3, the corresponding fingerprint data and position data of the

preceding fingerprint acquisition are read out and also supplied to the comparison device 4. The fingerprint features and their positions are compared there, and in the case of a correspondence which is within a tolerance range, the comparison device 4 evaluates the current fingerprint acquisition or, respectively, the current

identification process as misuse of fingerprint traces of the last identification process and rejects access which is indicated on a display device 6.

In this method, the invention is based on the fact that

(1) old fingerprint traces are no longer of consequence when a new arbitrary finger is placed on the area, and are replaced by the new print, and

(2) a user will not be able to position his finger, when placing it down again, with such accuracy that the finger corresponds to the preceding fingerprint within up to 100 µm or 50 µm in position and direction.

Since the position of the remaining traces of the earlier fingerprint of the preceding identification process cannot shift in space with respect to the sensor, it is not only the individual features of the fingerprint such as branches or minuscules but also their precise position on the contact area which are stored in the present invention, for example as xy coordinates or as polar coordinates. If, in the case of a new fingerprint of a new identification process, corresponding features lie within a tolerance range of 50 µm or 100 µm at the same spatial position, it is highly probable that this is not a new placement of a finger of the same person but the features of the last print. In this case, access authorization or identification must be refused and the user must be requested to place his finger again.

An exemplary embodiment of the method according to the invention will now be explained with reference to the flowchart of figure 2.

In a step S1, the biometric data and their associated positions on the contact area are acquired. In a step S2 these are stored for use

in the user identification process following next. In step 3, accordingly, the biometric data and associated positions of the preceding identification process are read out. In step S4, a comparison is made to determine whether the features and positions of the two successive acquisitions, i.e. the fingerprint acquisition of the current user identification process and the fingerprint acquisition of the immediately preceding user identification process correspond with each other. If both the features of the fingerprint have a defined degree of correspondence and the positions of these features correspond to one another within a tolerance range of 50 µm or 100 µm, the identification is refused (step S5), otherwise, the check continues to step S6 in which a check is made, as in known user identification methods, to determine whether the features of the current acquisition of the fingerprint correspond to the stored features of fingerprints of certain persons, for example authorized users. If this is not so, identification is refused (step S7), otherwise, identification takes place.

The variant of the method explained in figure 3 differs from that shown in figure 2 in that a mean value of the positions of acquired features of the biometric record (fingerprint) is calculated and stored in a step S11. In step S4, it is then not the positions of individual features of the fingerprints but the mean position values of the current fingerprint acquisition and the preceding one which are compared with one another. This has the advantage that statistic deviations due to stretching or compression of the skin or due to the pixel spacing of the contact area 5 of the fingerprint sensor are averaged out so that the tolerance range can be selected to be smaller, for example 10 µm to 20 µm. This reduces the probability of unjustified rejections of the identification.

The invention provides an improved method for biometric user identification in which misuse due to fingerprint traces of a preceding user identification which are remaining on the acquisition device can be prevented. The invention can be applied to checking the authorization to use devices such as, for example, mobile telephones or for identifying a computer user in bank transactions. However, other applications are also conceivable in which the identity of a person must be reliably established on the basis of biometric data such as, for example, a fingerprint.

Patent Claims

1. A method for biometric user identification having the following steps

(1) Acquisition of a biometric record of the user and the respective spatial position of the biometric data relative to a reference position,

(2) Storage of the biometric record and the associated position data,

(3) Reading out of the biometric record and the associated position data of a user identification process preceding the current user identification process,

(4) Comparison of the biometric data currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric data have a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range.

2. The method as claimed in claim 1, characterized in that the tolerance range is less than 100 µm, preferably about 50 µm.

3. The method as claimed in claim 1, characterized in that a mean value of the positions of a number of individual features of the biometric data is in each case determined and the positions of the mean values of two successive identification processes thus formed are compared in step (4).

4. The method as claimed in claim 3, characterized in that

the tolerance range is less than 50 µm, preferably between 10 µm and 20 µm.

5. The method as claimed in one of claims 1 to 4, characterized in that the biometric data are fingerprint data.

6. The method as claimed in claim 5, characterized in that, as position data, the coordinates of bifurcations or minuscules of the fingerprint on a contact area are determined.

7. The method as claimed in one of claims 1 to 6, characterized in that, after an identification process has ended, the stored data of the preceding identification process are deleted and overwritten by the data of the current identification process.

8. A device for biometric user identification, exhibiting
a device (1) for acquiring a biometric record of the user and of the respective spatial positions of the data relative to a reference position,
a memory (3) for storing the biometric data and the associated position data,
a comparison device (4) for comparing the biometric data and the associated position data of a current identification process with the biometric data and associated position data of a respective preceding identification process and for refusing the identification if the biometric data compared have a defined degree of correspondence and the positions of the corresponding biometric data correspond within a defined tolerance range.

9. The device as claimed in claim 8, characterized by an output device (6) for outputting the result of the user identification.

10. The device as claimed in claim 8 or 9, characterized in that the tolerance range is less than 100 µm, preferably about 50 µm.

11. The device as claimed in one of claims 8 to 10, characterized by a device (5) for calculating a mean value of the positions of a number of individual features of the biometric data and in which the comparison device (4) compares the positions of the mean values of corresponding features of successive user identification processes.

12. The device as claimed in claim 11, characterized in that the tolerance range is less than 50 µm, preferably between 10 µm and 20 µm.

13. The device as claimed in one of claims 8 to 12, characterized by a fingerprint sensor (1) for acquiring the fingerprint as biometric data and its position on a contact area (5) of the fingerprint sensor (1).

14. The device as claimed in claim 13, characterized in that the fingerprint sensor (1) determines the coordinates of certain features of the fingerprint on the contact area (5).

15. The device as claimed in claim 14, characterized in that

the features of the fingerprint are branches or minuscules.

16. The use of the method as claimed in one of claims 1 to 7 or of the device as claimed in one of claims 8 to 15 for checking the access authorization for the use of a mobile telephone or access to a computer network.

GR 99 P 1259

Abstract

User identification method

A method for biometric user identification exhibits the following steps:

(1) Acquisition of a biometric record of the user and the respective spatial position of the biometric data relative to a reference position,
(2) Storage of the biometric record and the associated position data,
(3) Reading out the biometric record and the associated position data of a user identification process preceding the current user identification process,
(4) Comparison of the biometric data currently acquired and associated position data with the preceding biometric data and associated position data read out and rejection of the identification if the biometric data have a defined degree of correspondence and the position of the corresponding biometric data corresponds within a defined tolerance range. The biometric data are preferably fingerprint data.

(Figure 2)

FIG 1

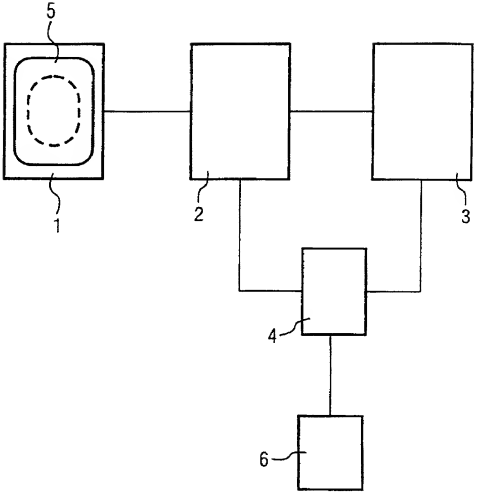


FIG 2

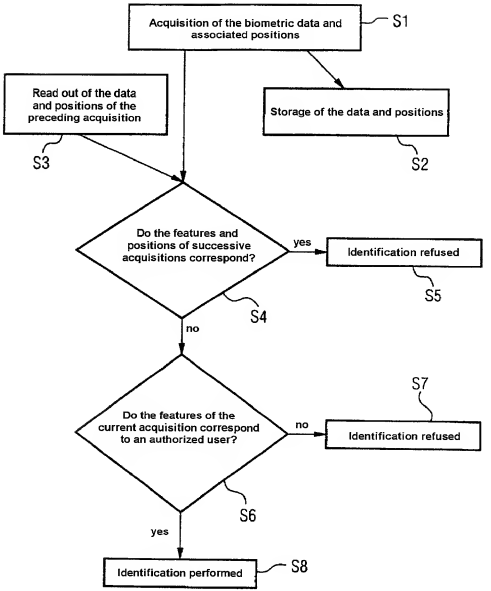
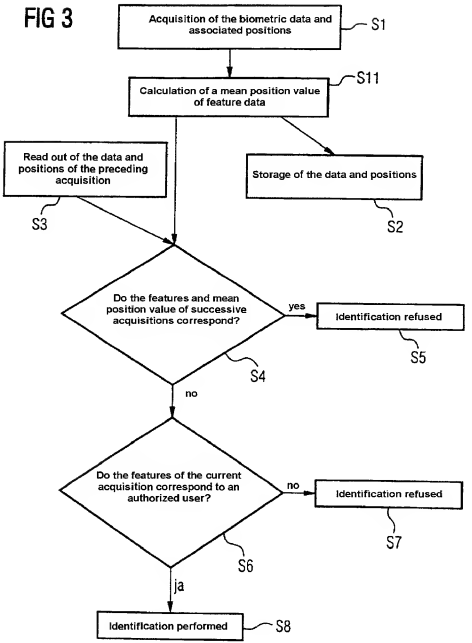


FIG 3



Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Benutzeridentifikationsverfahren

User identifcation method

deren Beschreibung

the specification of which

(zutreffendes ankreuzen)
☐ hier beigefügt ist.
☒ am 22.02.2000 als PCT internationale Anmeldung
PCT Anmeldungsnummer PCT/DE00/00492
eingereicht wurde und am _____
abgeändert wurde (falls tatsächlich abgeändert).

(check one)
☐ is attached hereto.
☒ was filed on 22.02.2000 as PCT international application
PCT Application No. PCT/DE00/00492
and was amended on _____
(if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

German Language Declaration

Prior foreign appplications
Priorität beansprucht

			Priority Claimed	
19907754.1 (Number) (Nummer)	DE (Country) (Land)	23.02.1999 (Day Month Year Filed) (Tag Monat Jahr eingereicht)	☒ Yes Ja	☐ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	☐ Yes Ja	☐ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	☐ Yes Ja	☐ No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE00/00492 (Application Serial No.) (Anmeldeseriennummer)	22.02.2000 (Filing Date D, M, Y) (Anmeldedatum T, M, J)	anhängig (Status) (patentiert, anhängig, aufgegeben)	pending (Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date D,M,Y) (Anmeldedatum T, M; J)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

(SEE ATTACHED SHEET)

Customer No.

And I hereby appoint

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

Ext. _____

Postanschrift:

Send Correspondence to:

Bell, Boyd & Lloyd LLC
Three First National Plaza, 70 West Madison Street, Suite 3300 60602-4207 Chicago, Illinois
Telephone: (001) 312 372 11 21 and Facsimile (001) 312 372 20 98
or
Customer No.

Voller Name des einzigen oder ursprünglichen Erfinders:	Full name of sole or first inventor:
Dr. MANFRED BROMBA	Dr. MANFRED BROMBA
Unterschrift des Erfinders Datum	Inventor's signature Date
Manfred Bromba 2001-07-10	
Wohnsitz	Residence
MUENCHEN, DEUTSCHLAND	MUENCHEN, GERMANY
Staatsangehörigkeit	Citizenship
DE	DE
Postanschrift	Post Office Addess
AM ISARKANAL 24	AM ISARKANAL 24
81379 MUENCHEN	81379 MUENCHEN
Voller Name des zweiten Miterfinders (falls zutreffend):	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum	Second Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Holby M. Abern (P47,372), Robert M. Barrett (30,142), Alan L. Barry (30,819), Thomas C. Basso (46,541), Jeffrey H. Canfield (38,404), Robert W. Connors (46,639), Amy J. Gast (41,773), James Jagoda (33,250), Patricia A. Kane (46,446), Michael S. Leonard (37,557), Edward A. Lehman (22,312), Adam H. Masia (35,602), Dante J. Picciano (33,543), Renato L. Smith (45,117), Maurice E. Teixeira (45,646), William E. Vaughan (39,056), Austin Victor (47,154), and all members of the firm of Bell, Boyd & Lloyd LLC.

William E. Vaughan
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690

William E. Vaughan
312.807.4292